moz://a

April 2023

# Mozilla's position on the EU's Cyber Resilience Act

## Introduction

Mozilla is a global community working together to build a better internet. As a mission-driven organization, we are dedicated to promoting openness, innovation, security, and accessibility online[1]. We are the creators of Firefox, an open-source browser that millions of Europeans use as their window to the web, as well as products like Mozilla VPN, Hubs, and the Pocket "read-it-later" application, used by hundreds of millions of individuals worldwide.

We believe that individuals' security and privacy online and a safe Internet overall can only be guaranteed when all actors comply with high cybersecurity standards. We are constantly investing in the security of our products, the internet, and its underlying infrastructure. Therefore, we welcome and support the overarching goals of the 'Cyber Resilience Act' (CRA) legislative proposal recently published by the European Commission.

Nevertheless, we would like to draw your attention to the inevitable unintended consequences the CRA can have if it remains in its current form. In this paper, we set out our perspectives and concrete recommendations for how lawmakers can improve the CRA during the upcoming legislative deliberations. To strike the right balance and achieve a legislative outcome that ultimately benefits internet users, we believe that EU policymakers should:

- Take into consideration the particularities of open-source software

[1] The Mozilla Manifesto - Pledge for a Healthy Internet

- Align the proposal with existing EU cybersecurity legislation & ensure that cybersecurity risks will not be amplified by introducing obligations to report unmitigated vulnerabilities

## Clarifying 'commercial activity' for open-source software

Mozilla strongly believes that free and open software promotes the development of the internet as a public resource[2]. According to a European Commission study (2021), organizations in the EU invested about €1 billion in open-source software only in 2018, with an estimated impact on the European economy of between €65 and €95 billion. The same study highlights that open source contributes significantly to the EU's GDP. Therefore, we welcome the European Commission's support over the past years in open-source projects and software development. With its renewed Open Source Software Strategy, the EU's executive has shown its commitment to promoting the development of open-source software solutions. Open source software is often developed by individuals or small teams of part-time contributors who raise costs only to pay for the maintenance of the software rather than making a profit from its sale.

The CRA, however, is an example of a legislative proposal contrary to the abovementioned strategic direction by the European Commission. The coverage of open-source software that indulges in commercial activity, as stipulated in *Recital 10*, can only have a little positive effect on the open-source community. Many open-source projects do not operate in a strict business context, nor are they developed for commercial purposes, as non-profit organizations drive them. The wide definition of "commercial activity" ends up encapsulating many models of open source development that cannot handle the compliance of a dense law like the Cyber Resilience Act. Unintentionally including them under the CRA obligations will overly burden such projects, disincentivizing investments and eventually shrinking the open source pool with a direct impact on the European economy.

To be more precise, there are instances where a charge for technical support is necessary and needed to cover the costs incurred from running such projects. As *Recital 10* currently stands, such an activity (charging consumers for technical support) will automatically and unintentionally capture a large part of independent open-source projects. Moreover, it is unclear under the current wording if projects that receive financial donations from business entities or companies for their open-source work will be deemed as operating in a commercial context.

Overall, we acknowledge and support the Commission's intention to cover all commercial activities under the CRA. Therefore, should an open-source project have evidently commercial and profit-making characteristics, it should also be covered by the CRA. What we do believe, though, is that projects which only receive revenues to fund their financial existence should not be

[2] Principle 7 - Mozilla Manifesto

considered a commercial activity[3] (e.g., revenues stemming from charging a small fee for the technical support of the freely provided software, revenues from search, donations, etc.)

This idea is not novel and is already part of the EU acquis. Directive 2019/770 on the supply of digital content and digital services[4] already provides safeguards for open-source projects in Recital 32. It specifically states that "*free and open-source software can contribute to research and innovation in the market for digital content and digital services*." For that reason and to avoid imposing obstacles to market development, Directive 2019/770 does **not apply** to free and open-source software, *provided that it is not supplied in exchange for a price* and that the *consumer's personal data are exclusively used for improving the security, compatibility or interoperability of the software*.

*Recommendations*

- We propose clarifying and narrowing the scope of what constitutes a commercial activity. Therefore, **Recital 10** should be amended as follows:
  - (...)In the context of software, a commercial activity ***solely occurs when a price is charged for the use of a product with the intention of making a profit*** or by providing a software platform through which the manufacturer monetizes other services, or by the ***monetization of personal data*** for reasons other than exclusively for improving the security, compatibility or interoperability of the software.
- To enhance legal clarity for the open source community, we also ask legislators to explicitly add the above-mentioned exception in **Article 2, paragraph 5b.** Specifically, we recommend explicitly stating that open-source projects that are not supplied in exchange for a price or data monetization should be excluded from the CRA's scope:
  - **Art 2, para 5(b):** *This Regulation does not apply to free and open-source software, including its source code and modified versions, except when such software is provided in exchange for a price or as a monetized product with the intention of making a profit rather than performing maintenance."*

## Aligning the CRA with existing EU rules & minimizing risks from reporting unmitigated vulnerabilities

The CRA has been widely seen as the last missing piece regarding EU cybersecurity policies and standard-setting. Being part of the EU's effort to tackle cybercrime and protect consumers from

[3] It is important to note that we acknowledge that Mozilla and our open-source products do fall under the definition of 'commercial activity.' We do not wish or claim that Mozilla and similar organizations operating in a business context should be exempted from the CRA. However, we do believe that there are other organizations, part of the open-source community, that will unintendedly be covered by the CRA.

[4] Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services

cyber incidents, the CRA should be closely aligned and linked with other major cybersecurity legislation the EU managed to approve in the past years, such as the NISD2 *(Directive (EU) 2016/1148)*.

The current proposal from the European Commission is failing to achieve this alignment, particularly in the areas of incidents and reporting. It is paramount to harmonize the obligations under the already adopted NISD2 and the CRA proposal. Such an alignment will help all players, irrespective of their size and resources, to comply with the rules. At the same time, it will not create unnecessary confusion with regard to competent authorities as well as overly burden the resources of said authorities.

To be more precise, we are concerned about how vulnerability reporting obligations (and specifically Article 11) will apply in practice. Reading the Commission's proposal, we understand that there is a clear risk from disclosing unmitigated vulnerabilities, which eventually can undermine the very purpose of the CRA. Furthermore, conducting such reporting in different timeframes for the NISD2 and the CRA can only create further confusion.

At Mozilla, we have long advocated for reforms to how governments handle vulnerabilities. Indeed, governments have been known to stockpile vulnerabilities and use vulnerabilities rather than disclose them. Such stores of vulnerabilities can be abused by governments themselves. They can also be a target for malicious third parties; government stockpiles in the past have leaked online or been stolen, resulting in global cybersecurity incidents that cost lives and billions of euros. Thus any provision of the CRA that would require companies to share unpatched vulnerabilities needs to be scrutinized carefully. Indeed, we believe that as a general policy, sharing unpatched vulnerabilities with governments should be discouraged and, even if well intended, creates more risk than it solves.

Article 11 of the CRA proposal requires manufacturers to notify ENISA of any *actively exploited vulnerabilities* in their products within 24 hours. The way paragraph 1 of this Article is drafted suggests that manufacturers will have to report also unmitigated (or unpatched) vulnerabilities. This is quite concerning considering that it can undermine existing industry standards as well as, more importantly, create risks of using the disclosure of such unpatched vulnerabilities for malicious purposes by certain actors. Applying corrective measures is of high priority when vulnerabilities occur. Therefore, it is an existing best practice to involve only the actors needed to resolve the vulnerability. Obliging manufacturers to report to ENISA within such a tight timeframe can only undermine the efforts taken to apply corrective measures and reflects a misunderstanding of how long it takes for these vulnerabilities to be fixed. At the same time, creating a centralized database or registry of unmitigated vulnerabilities (even if maintained by ENISA) only has added value for malicious actors that will try to access and exploit such a similar registry (for example, the Log4j vulnerability). Ensuring that such information is shared in line with strict security protocols or on a need-to-know basis, as some have suggested, has little value and will not address this underlying risk.

*Recommendations*

Mozilla urges EU policymakers to consider the above when amending Article 11 and the relevant reporting obligations for manufacturers. Given the different sizes and compliance capabilities of manufacturers of products with digital elements covered under the CRA, we specifically ask the co-legislators to

- **Refocus Article 11 only on reporting mitigated vulnerabilities** - to avoid further cybersecurity risks and the possibility of malicious actors exploiting reported, unmitigated vulnerabilities, paragraph 1 should ensure that it creates the necessary conditions for reporting to ENSIA only vulnerabilities that have already been patched.
- **Ensure reporting obligations focus on vulnerabilities posing 'significant risks'** - the existing threshold is too low [Art 11(1): *"...notify...any actively exploited vulnerability"*)], and it risks creating an overflow of low-severity incidents which will result in administrative burden both for manufacturers and reporting authorities
- **Align incident reporting timelines & authorities with NISD2** - for entities covered under both NISD2 and CRA, two different timelines seem to apply. The incident reporting timeline for NISD2 is 72 hours, while for CRA, it is 24 hours. This discrepancy can lead to confusion and a lack of legal clarity. Thus we ask policymakers to align the CRA timeline from 24 to 72 hours, as is the case for NISD2.

Concrete amendment to Article 11(1):

- *The manufacturer shall notify ENISA of any actively exploited vulnerability contained in products with digital elements* ***that present a significant cybersecurity risk. Such notification should occur without undue delay and, in any event, within 72 hours from the moment corrective measures to mitigate the vulnerability have been made available.*** *The notification shall include details concerning that vulnerability and, where applicable,* ***the corrective or mitigating measures taken****. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability.*

## About Mozilla

Mozilla is the public benefit technology company and maker of the open-source Firefox web browser, Mozilla VPN, and the Pocket "read-it-later" application. Mozilla Corporation is a private company fully owned by its sole shareholder, the non-profit Mozilla Foundation. The Mozilla Foundation furthers our mission to protect an open and accessible internet by investing in advocacy, research, and movement-building. It is guided by the set of principles in the Mozilla Manifesto that recognize, among other things, that the internet must remain open and accessible; and that security and privacy are fundamental.

*For more information, please contact Tasos Stampelos (tstampelos@mozilla.com) or Udbhav Tiwari (utiwari@mozilla.com), Mozilla Corporation*